SL

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/728,257	12/01/2000	Chad Schoettger	P5402	3873

32658 7590 06/21/2004

HOGAN & HARTSON LLP
ONE TABOR CENTER, SUITE 1500
1200 SEVENTEEN ST.
DENVER, CO 80202

EXAMINER	
POLTORAK, PIOTR	

ART UNIT	PAPER NUMBER
2134	6

DATE MAILED: 06/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

SL

Office Action Summary	Application No.	Applicant(s)	
	09/728,257	SCHOETTGER, CHAD	
	Examiner	Art Unit	
	Peter Poltorak	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 December 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 2.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-22 have been examined on the merits.

Priority

1. No claim for priority has been made in this application.
2. The effective filing date for the subject matter defined in the pending claims in this application is 12/01/2000.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 19-22 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Computer programs and code must be embodied on computer readable media.

Claim Objections

4. Claim19 objected to because of the following informalities: the second limitation recites, "to verify **the** that the exterior device..."(emphasis added). The first "the" within the cited part of the limitation is unnecessary. The applicant is advised to check all the claims for other possible grammatical errors.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 7-8, 15,17, 19, and 21-22 and dependent claim 20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

7. Claims 7 and 8 contradict each other. Claim 7 states the limitation " the method ... further including examining the response for an error message, translating the error message, and including the error message in the response transmitted to the external client", and it's dependent claim 8 recites "to take corrective actions to remove the error message from the response from the computer device".

8. Claims 15 and 17, contain the trademark/trade name "Java". Where a trademark or trade name is used in a claim as a limitation to identify or describe a particular material or product, the claim does not comply with the requirements of 35 U.S.C. 112, second paragraph. See Ex parte Simpson, 218 USPQ 1020 (Bd. App. 1982). The claim scope is uncertain since the trademark or trade name cannot be used properly to identify any particular material or product. A trademark or trade name is used to identify a source of goods, and not the goods themselves. Thus, a trademark or trade name does not identify or describe the goods associated with the trademark or trade name. In the present case, the trademark/trade name is used to identify/describe a computer language and, accordingly, the identification/description is indefinite.

9. The term "computer code devices" as used in claims 19 and 21-22 does not allow the examiner to determine whether it is directed towards computer code or towards a computer device.

Appropriate corrections are required.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. *Claims 1-22* are rejected under 35 U.S.C. 103(a) as being unpatentable over Luckenbaugh et al. *(U.S. Patent No. 6,311,269)* in view of Lincoln D. Stein, "Web Security, "A step-by-step reference Guide, ISBN 0-201-63489-9, 1998 and further in view of Marty Hall, "Servlets and JSP: An Overview" http://web.archive.org/web/20000511042158/http://www.apl.jhu.edu/~hall/java/Servlet-Tutorial/Servlet-Tutorial-Overview.html, 1999 and Bisaillon et al., TCP/IP With Windows NT Illustrated, ISBN 0-072-12910-7, 1998.

12. Luckenbaugh et al. teach an external client *(Web Browser 30, Fig. 1)* with selective access to a computer device *(storage 60, Fig. 1)* protected behind a host comprising:

providing a tunnel mechanism *(CGI, col.5 lines 65-67 and col. 6 lines 1-18)* between the host and the computer device, wherein the tunnel

mechanism is in communication with the host *(Fig. 4 object 50)* and the computer device *(Fig. 4 step 14);*

receiving with the tunnel mechanism an access request to the computer device from the external client *(Fig. 4 step 1 and 2)*;

verifying the external client currently has authorized access to the host *(Abstract)*; and after successful completion of the verifying routing, authorization to the host routing client's request to the computer device *(Abstract).* Luckenbaugh et al. also teach a method for controlling access to a device *(storage 60, Fig. 1)* by a client device *(Web Browser 30, Fig. 1)* on an external data communications network, the method comprising: receiving with a tunnel mechanism *(CGI)* an access request from the external client device to the internal network device *(Fig. 4 step 1 and 2)*, the tunnel device being communicatively linked with an interface of the internal device *(Fig. 4 step 14)*, receiving a response to the modified access request from the internal device at the tunnel mechanism *(Fig. 4 step 14).* Luckenbaugh et al. further teach the method wherein the internal network includes a plurality of internal devices *(Web Browser 30 and storage 60, Fig. 1)*, and the access request modifying includes determining a destination interface for one of the internal devices wherein the access request includes URL information *(Fig.2 object 211)* and the access request modifying the URL information includes URL information for the internal device *(Col. 8 lines13-30)*, and verifying that the internal

device is authenticated as an authorized user of a host device prior to the request routing *(abstract)*.

13. Luckenbaugh et al. also teach establishing a communicative link between the tunnel mechanism and the destination interface *(Fig. 4 sep 14)*, and the method wherein the modifying the response to include identification information for the tunnel mechanism to the response *(cookie, col. 5 lines 14-31, col. 6 lines 34-44)*, the response including URL information *(Fig. 4 step 11)* and the added identification information includes URL information for the tunnel mechanism *(col. 8 lines 17-30)*, and the routing including limiting the access request to the computer device to the determined level of the authorized access *(col. 3 lines 16-22)*. Although Luckenbaugh et al. do not explicitly teach modifying the access request to include an address of the interface of the internal device, and modifying the response prior to transmitting it to the external client to remove identification information for the computer device. However these features are taught Luckenbaugh et al. (in view of Bisaillon) as lines 50-63 of column 7 and col. 5 lines 14-31 show that only the tunnel mechanism can retrieve location of and communicate with the internal device *(secured HTML)*. Thus the internal device address is not known to the remote client and at each transaction it is added in order for the request to reach the destination. *Bisaillon et al.* teach that HTTP operates using TCP/IP (*Bisaillon et al. pg. 41, Figure 1-33*) where the web name is resolved into an IP address (*Bisaillon et al. pg.448, steps 1-2*), and that HTML is accessed using HTTP (*Bisaillon et al. pg.448*). Furthermore, Bisaillon et al.

teach that TCP header contains internal device identification information *(source information, pg. 14, Figure 1-10)*. It would be obvious to one of ordinary skill to remove the identification information of the internal device prior to transmittal of the modified response to the external client device in order to minimize the threat of accessing secure HTML by an external client directly. As pointed out in the second paragraph of 35 U.S.C. 112 rejection claims 7-8 are read as contradictory to each other. However, the examiner believes that Luckenbaugh's et al. objects 313-314 of Fig. 3A would render the claims obvious. Luckenbaugh et al. also teach that the host device is a HTTP Web *(*Luckenbaugh et al., *Fig. 1)* and that the tunnel mechanism comprises CGI. However, he does not explicitly teach that the server is configured to support JAVA and the tunnel mechanism comprises a Java servlet. Hall teaches that Java servlets are more efficient, easier to use, more powerful, more portable, and cheaper than traditional CGI *(Hall, What are the Advantage of Servlets Over "Traditional" CGI?)*. Therefore it would be obvious to one of ordinary skill in art at the time of the invention to support and implement Java servlets as the tunnel mechanism to increase the overall transaction efficiency.

14. Luckenbaugh et al. do not explicitly teach protecting the computer device with the firewall. Luckenbaugh et al. also do not explicitly teach modifying the access request to include an address of the interface of the internal device, operating the tunnel mechanism to route the modified access request to the interface of the internal device, and modifying the response with the tunnel mechanism to

remove the identification information prior to transmittal of the modified response to the external client device. However these features are anticipated by Luckenbaugh et al. (in view of Bisaillon et al.) as lines 50-63 of column 7 and col. 5 lines 14-31 show that only the tunnel mechanism can retrieve location of and access the secured HTML. Thus the internal device address is not known to the remote client and it would have to be added in order for the tunnel mechanism to receive the response as it is shown in Fig. 4 step 14. *Bisaillon et al.* teach that HTTP operates using TCP/IP (*Bisaillon et al. pg. 41, Figure 1-33*) where the web name is resolved into an IP address (*Bisaillon et al. pg.448, steps 1-2*), and that HTML is accessed using HTTP (*Bisaillon et al. pg.448*). Furthermore, Bisaillon et al. teach that TCP header contains internal device identification information *(source information, pg. 14, Figure 1-10)*. It would be obvious to one of ordinary skill in art to remove the identification information of the internal device prior to transmittal of the modified response to the external client device in order to minimize the threat of accessing a secure HTML by an external client directly. Luckenbaugh et al. further do not explicitly teach the tunnel mechanism being communicatively linked to the firewall and an interface of the internal device. Stein teaches that firewall systems provide security to organization in order to prevent outside attacks *(Stein pg. 387)*. Therefore it would be obvious to one of ordinary skill in art at the time of the invention to protect corporate resources by restricting the direct communicative link between inside resources (including the

tunnel mechanism) and the remote clients and utilize the communication via a firewall as taught by Stein.

15. Stein teaches that firewall systems provide security organizations in order to prevent outside attacks *(Stein pg. 387)*. Therefore it would be obvious to one of ordinary skill in art at the time of invention was made to implement a firewall between the external client and inside resources to protect corporate resources such as hosts and other computer devices.

16. **Claims 1- 4, 9, 16, 18 and 18-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bal et al. *(U.S. Patent No. 6,457,061)* in view of Lincoln D. Stein, "Web Security, "A step-by-step reference Guide, ISBN 0-201-63489-9, 1998 in light of Harry Newton, "Newton's telecom dictionary. The official dictionary of telecommunications & the Internet", ISBN 1-57820-023-7, 1998 and Finley *(U.S. Patent No. US 5,815,571)*.**

17. *Bal at al.* teach network address translation that changes external addresses to internal addresses and internal to external addresses (pg. 3 lines 54-58 and col. 4 lines 25-50). *Newton* teaches that tunneling means to temporarily change the destination of a packet in order to traverse one or more routers that are incapable of routing to the real destination (pg. 787-789). Thus Bal et al teach implementing network access translation as a tunneling mechanism to alleviate routing restriction within the network environment on network communication. Bal et al. also teach a method for providing an external client (Fig. 2, Internet 100 node) with selective access to a computer device (Fig. 2, LAN 140 node)

protected behind a host (Fig. 2, object 230). Tunnel mechanism (implemented in network address translation) is in communication with the host and the computer device. The tunnel mechanism receives an access request to the computer device from the external client as lines 9-13 col. 4 show that all the communication passes through the tunnel mechanism and as Fig. 2 shows the tunnel mechanism implemented on the host. Thus each request from an external client directed to a computer device is received by the tunnel mechanism before reaching the destination.

18. Bal et al. do not explicitly teach protecting the computer device with the firewall, authorizing clients to access any interior nodes, determining a level of the authorized access and, routing to the computer device the determined level of the authorized access. Bal et al. also do not explicitly teach establishing a communicative link between the tunnel mechanism and the destination interface; however since tunnel mechanism (network address translation) is responsible for changing the destination address it would be obvious to one of ordinary skill in art to employ the tunnel mechanism to establish link with the destination interface, assuring that the device is operational and available to receive requests. In result network address translation would be utilized to minimize unnecessary traffic.

19. Stein teaches that firewall systems provide security to organization in order to prevent outside attacks *(Stein pg. 387). Stein* teaches that all traffic from the outside world first goes through the firewall *(Stein pg. 387, § 2 and 388, § 1)*,

which decides whether the traffic can be allowed through. Therefore it would be obvious to one of ordinary skill in art at the time of invention to implement a firewall between the external client and inside resources to protect corporate resources such as hosts and other computer devices. The verifying the external client access request and routing the message upon successful completion of the verifying to the computer device is inherent in Stein's teaching, as it is that the message after successful completion of the verifying access request is routed to the device with the tunnel mechanism since all communication goes first through the host (Bal et al., col. 4 lines 10-12 and lines 42-50) and as a result the tunnel mechanism would be used to get the message to the destination of Bal's et al. teaching.

Finley teaches that any computer system which has external connections is subject to attack and that the damage to the systems would depend on the authorization level at which the hacker logs on *(col. 1 lines 6-12)*. Thus it would be obvious to one of ordinary skill in art to implement various levels of the authorized access, and routing requests based on the level in order to issue the highest privileges only to the most important parties e.g. administrators.

20. **Claims 7-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bal et al. *(U.S. Patent No. 6,457,061)* in view of Kelley *(U.S. Patent No. 6,526,524)* and further in view of Dow et al. *(U.S. Patent No. 6,441,927).***

21. Bal et al. is described supra.

22. Bal et al. do not explicitly teach examining for an error message, translating and taking corrective action by removing the error message and including the error message in the response transmitted to the external client.

23. Kelley teaches examining for and translating errors and taking corrective actions to remove the error message (Kelley, pg. 3 lines 10-30). Dow et al. teaches including the error message in the response transmitted to the external client (Dow et al., pg. 8 lines 7-21). It would be obvious to one of ordinary skill in art to implement Kelley's and Dow's et al. teaching in Bal et al.'s invention in order to quickly address error message and improve applications as well as keeping clients informed and as a result keeping them satisfied.

24. **Claims 10-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bal et al. *(U.S. Patent No. 64,457,061)* in light of Harry Newton, "Newton's telecom dictionary. The official dictionary of telecommunications & the Internet", ISBN 1-57820-023-7, 1998 in view of Linclon D. Stein, "Web Security, "A step-by-step reference Guide, ISBN 0-201-63489-9, 1998**

Bal at al. teach network address translation that changes external addresses to internal addresses and internal to external addresses (pg. 3 lines 54-58 and col. 4 lines 25-50). *Newton* teaches that tunneling means to temporarily change the destination of a packet in order to traverse one or more routers that are incapable of routing to the real destination (pg. 787-789). Thus it would be obvious to one of ordinary skill in art to implement network access translation as a tunneling mechanism to alleviate routing restriction within the network environment on

network communication. Bal et al. further teach a method for controlling access to a device (Bal et al., Fig. 2, LAN 140 node) on an internal network including a plurality of the internal devices Bal et al. Fig. 1) by a client device on an external data communication network (Bal et al., Fig. 2, Internet 100 node). Bal et al. also teach that all internal/external communication must pass through the tunnel mechanism (Bal et al., network address translation col. 4 lines 10-13) and that the tunnel mechanism must change the addresses for the data to reach the destination (Bal et al., col. 4 lines 42-50). In other words the tunnel mechanism in Bal et al. receives all internal/external access requests, translating the address from internal to external (or external to internal) and forwarding the translated packets to their destination (Bal et al., col.11 lines 52-55 and pg. 9 lines 28-44, Fig. 7 for example).

Bal et al. do not teach protecting the computer device with the firewall.

Stein teaches that firewall systems provide security to organization in order to prevent outside attacks *(Stein pg. 387).* Therefore it would be obvious to one of ordinary skill in art at the time of invention to implement a firewall between the external and internal network devices to protect corporate resources.

25. **Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bal et al. *(U.S. Patent No. 64,457,061)* in light of Harry Newton, "Newton's telecom dictionary. The official dictionary of telecommunications & the Internet", ISBN 1-57820-023-7, 1998 and in view of Linclon D. Stein, "Web Security, "A**

step-by-step reference Guide, ISBN 0-201-63489-9, 1998, and Bisaillon et al., TCP/IP With Windows NT Illustrated, ISBN 0-072-12910-7, 1998

26. *Bal at al.* teach network address translation that changes external addresses to internal addresses and internal to external addresses (pg. 3 lines 54-58 and col. 4 lines 25-50). *Newton* teaches that tunneling means to temporarily change the destination of a packet in order to traverse one or more routers that are incapable of routing to the real destination (pg. 787-789). Thus it would be obvious to one of ordinary skill in art to implement network access translation as a tunneling mechanism to alleviate routing problems.

27. Bal et al. further teach a method for controlling access to access to a computer device (Fig. 2, LAN 140 node) on an internal network, a tunnel mechanism linked to the computer device adapted for modifying the request to include an address of an interface of the computer device (pg. 9 lines 28-44, Fig. 7, claim 4 in col. 11 lines 52-55), routing the modified request to the computer device (col. 11 lines 52-55). Bal et al. also teach that all communication goes through the host (Bal et al., col. 4 lines 10-12 and lines 42-50), and it is inherent that a host server on an interior side of the firewall is linked to the firewall and thus configured for receiving a request from a client device located exterior to the firewall.

28. Bal et al. do not explicitly teach receiving a response from the computer device including identification information device. However, *Bisaillon et al.* teach that in the TCP/IP communication a response from the computer device includes identification information (source information, *Bisaillon et al., pg. 14, Figure 1-10*)

and furthermore they underline that that tunnel mechanism uses an internal Internet Protocol address when communication with nodes on the internal local area network and external Internet Protocol address when communicating with nodes on the global Internet (Bal et al. pg. 5 lines 15-35). It would be obvious to one of ordinary skill in art to remove the identification information prior to transmittal of the modified response to the external client device (exchange internal IP address with the external one when sending a response from the internal computer device to external client device when utilizing the network address translation) to avoid possible communication errors. Also, Bal et al. do not explicitly teach protecting the computer device with the firewall and do not teach a host server on an interior side of the firewall the host server being linked to the firewall and configured for receiving a request from a client device located exterior to the firewall.

29. Stein teaches that firewall systems provide security to organization in order to prevent outside attacks *(Stein pg. 387)*. *Stein* teaches that all traffic from the outside world first goes through the firewall *(Stein pg. 387, §2 and 388, § 1)*, which decides whether the traffic can be allowed through. Therefore it would be obvious to one of ordinary skill in art at the time of invention to implement a firewall between the external client and inside resources to protect corporate resources such as hosts and other computer devices. Appropriate corrections are required.

Conclusion

No claim is allowed.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (703) 305-0719. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Signature

Date

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100